What Is Claimed Is:

1. A security access service method in processing member login in an on-line service, comprising:

an authentication step by the input of text;

an access location tracking step;

an authentication step by the input of coordinates; and

an access history report step.

2. The security access service method as claimed in claim 1, wherein the access location tracking step is performed between the two authentication steps.

3. The security access service method as claimed in claim 1, wherein the access history report step includes the steps of:

if another access is attempted with a user being already accessed, comparing the location of a person who attempts access, which is obtained in the access location tracking step, with the access location of a current login status, and if the location of the user and the access location of the current login status are different, immediately reporting the access location of the person who attempts access to the user of the current login status through a screen, and

if the location of the user and the access location of the current login status are the same, the obtained positional information of the person who attempts access is always reported to the user upon next logging in.

4. The security access service method as claimed in claim 1, wherein the access history report step includes the step of, if the authentication step by the input of the coordinates fails, immediately sending an alarm message through message means that is designated by the user.

5. A security access service method in processing member login in an on-line service, comprising:

an authentication step by the input of text; and

an authentication step by the input of coordinates.

6. The security access service method as claimed in any one of claims 1 to 5, wherein the authentication step by the input of the coordinates comprises the steps of:

transmitting an image table in which a key image is randomly mixed with a plurality of other images to the screen of the user;

manipulating the entire images to have the same value at the same time according to a manipulation value of a keyboard or a mouse of the user;

confirming a position manipulated by the key image; and

if coordinates whose manipulation of a position is confirmed and key coordinates previously designated by the user coincide with each other, determining that authentication is successful, and if they do not coincide with each other, determining that that authentication is unsuccessful.

7. The security access service method as claimed in claim 6, wherein the key coordinates are positions designated using a second key image.

8. The security access service method as claimed in claim 7, further comprising the step of, if a first key image passes through a position designated by a booby trap key image through the manipulation of the user, determining that authentication is unsuccessful, and transmitting an alarm message to a PC of the user or an original owner of an ID.

9. The security access service method as claimed in claim 7, further comprising the steps of, if the user places the first key image at a position designated by a report key image and then confirms the manipulation, determining that authentication is successful, and allowing this fact to be automatically reported through a guard system.

10. A method of safely authenticating a user, comprising the steps of:

transmitting an image table in which a key image is randomly mixed with a plurality of other images to a screen of a user;

manipulating the entire images to have the same value at the same time according to a manipulation value of a keyboard or a mouse of the user;

confirming a position manipulated by the key image; and

if coordinates whose manipulation of a position is confirmed and key coordinates previously designated by the user coincide with each other, determining that authentication is successful, and if they do not coincide with each other, determining that that authentication is unsuccessful.

11. The safe authentication method as claimed in claim 10, wherein the key coordinates are positions designated using a second key image.

12. The safe authentication method as claimed in claim 11, further comprising the step of, if a first key image passes through a position designated by a booby trap key image through the manipulation of the user, determining that authentication is unsuccessful, and transmitting an alarm message to a PC of the user or an original owner of an ID.

13. The safe authentication method as claimed in claim 11, further comprising the steps of, if the user places a first key image at a position designated by a report key image and then confirms the manipulation, determining that authentication is successful, and allowing this fact to be automatically reported through a guard system.

14. The safe authentication method as claimed in any one of claim 1 to 9, further comprising the step of registering a

personalization image table in which a construction image history of provided image tables is differently registered on a user basis.

15. The safe authentication method as claimed in claim 14, wherein the step of registering the personalization image table comprises the steps of:

allowing the user to select a key image and a through coordinate image or a terminal coordinate image from a group of images, which are much more than the number of images that are required in the personalization image table, and then to input the selected images;

allowing a server to randomly extract images as many as the number of images, which is necessary to complete the image table, from the remaining images except for the selected images; and

mixing the images that are selected and inputted by the user and the images that is selected by the server, and registering the personalization image table.

16. The safe authentication method as claimed in any one of claims 10 to 13, further comprising the step of inputting a text password, and

wherein the authentication process step includes determining that authentication is successful only when both the text password and the key coordinate are valid after the input of the text password and the key coordinates has been completed, and determining that authentication is unsuccessful if either

the text password or the key coordinate is not valid.

17. The safe authentication method as claimed in any one of claims 1 to 9, 14 and 15, further comprising:

a key coordinate registration step of providing the interface for allowing the user to differently define key coordinates for a main computer and key coordinates for a strange computer, and registering the inputted information;

a terminal information acquisition step of acquiring recognized information of a computer of the user;

a terminal recognition step of determining the computer as the main computer or the strange computer based on the recognized information on the computer of the user, which is acquired in the terminal information acquisition step;

a main computer registration step of, if it is determined that the computer is the strange computer in the terminal recognition step, registering the computer information to provide a main computer registration interface that can be registered as the main computer, and registering the inputted information; and

a strange computer alarm step of, if the computer is determined to be the strange computer in the terminal recognition step, notifying the user of the alarm message regardless of the authentication result,

wherein the authentication step by the input of the coordinates includes determining whether the coordinates the manipulation of the position of which is confirmed and the key

coordinates previously designated by the user coincide with each other, if the computer is determined to be the main computer in the terminal recognition step, confirming the key coordinates for the main computer, and if the computer is determined to be the stranger computer in the terminal recognition step, confirming the key coordinates for the strange computer.

18. The safe authentication method as claimed in claim 17, wherein the key coordinates are two or more, and all the key coordinates are confirmed in the strange computer, and only some of the key coordinates are confirmed in the main computer.

19. A method of safely authenticating a user, comprising the steps of:

a password registration step of providing the interface for allowing a user to differently define passwords for a main computer and passwords for a strange computer, and storing the inputted information;

a terminal information acquisition step of acquiring recognized information of a computer of the user;

a terminal recognition step of determining the computer as the main computer or the strange computer based on the recognized information of the computer of the user, which is acquired in the terminal information acquisition step;

a main computer registration step of, if it is determined that the computer is the strange computer in the terminal recognition step, registering the computer information to

provide a main computer registration interface that can be registered as the main computer; and

an authentication processing step of, if the computer is determined the main computer in the terminal recognition step, confirming a password for the main computer, and if the computer is determined the strange computer in the terminal recognition step, confirming a password for the strange computer.

20. The safe authentication method as claimed in claim 19, further comprising the steps of:

providing the interface for allowing the user to register a contact point where the alarm message is received, and storing the inputted information; and

a strange computer alarm step of, if the computer is determined to be the strange computer in the terminal recognition step, notifying the alarm message to the contact point regardless of the authentication result.